ISSN 1392 – 1215 ELEKTRONIKA IR ELERKTROTECHNIKA. 2005. Nr. 4(60)

T 180 TELEKOMUNIKACIJŲ INŽINERIJA

Neuroninių tinklų naudojimas kompiuterinių virusų sukeliamoms epidemijoms aptikti

D. Puniškis
Elektronikos inžinerijos katedra, Kauno technologijos universitetas,
Studentų g. 50, LT-51368 Kaunas, Lietuva, el.p. danius.puniskis@stud.ktu.lt
R. Laurutis
UAB „Informacijos alėja“, Dvaro g. 55, LT-76344 Šiauliai, Lietuva, el.p. remigijusl@aleja.lt

Įvadas

Perduodamų duomenų kiekis kasmet didėja didžiuliais tempais, daugėja tiek telekomunikacijų paslaugų teikėjų, tiek jų teikiamų paslaugų. Saugomai ir tinklais perduodamai informacijai tampant vis didesniu turtu, vienas iš svarbiausių kriterijų, naudojantis telekomunikacijų tinklais, tampa saugumas.

ISCA Labs apklausoje (2002 m.) dalyvavo 933 918 kompiuterių vartotojų. Šios apklausos duomenimis, per pastaruosius 5 metus duomenų užkrėtimų virusais skaičius padidėjo dvylika kartų – nuo 10 iki 125 infekcijų tūkstančiui kompiuterių per mėnesį, nors 96 % apklaustųjų naudojo standartines antivirusines programas [1,2].

Kompiuteriniai virusai yra pripažįstami pirmojo dirbtinio intelekto atstovais. Būtent jie pirmieji iš žmonių sukurtų kūrinių sugeba savarankiškai gyvuoti, daugintis, mutuoti ir vykdyti jiems užprogramuotas funkcijas.

Dėl kompiuterinių ir biologinių virusų analogijos, kovos metodai ir būdai su kompiuteriniais virusais išlieka panašūs kaip ir medicinoje su biologiniais virusais. Yra du iš esmės skirtingi požiūriai į biologinę virusologiją ir kovos su biologiniais virusais būdai [4] :

- mikroskopinis būdas;
- makroskopinis būdas.

Kompiuterinių virusų aptikimo metodikos

Virusai el.pašto tinklą dažniausiai naudoja dauginimuisi o kartu ir įrangai infekuoti [2]. Paprastai virusai surenka daug vartotojų adresų ir jiems siunčia savo kopijas, kad vartotojų kompiuteriuose vėl atliktų tą patį veiksmą – rastų naujų adresų ir jiems išsiųstų savo kopijas. Adresai gali būti randami elektroninėse adresų knygelėse ar nuskaitant tinklo srautą.

Antivirusinės sistemos, veikiančios šablonų atpažinimo metodu, priskiriamos mikroskopinėms sistemoms. Jos tikrina laiškus ir seka, ar juose nėra baitų sekos, sutampančios su žinomų virusų baitų sekomis. Jei antivirusinis skaitytuvas neturi duomenų apie kenkėjišką programą, jis nesugebės kovoti su ja. Dėl šios priežasties šablonines antivirusinių sistemų šablonų duomenų bazes reikia dažnai atnaujinti.

Kitaip nei mikroskopinės, kompiuterių makroskopinės virusologijos principai yra prastai ištyrinėti. Iš esmės tai lemia didelė techninės įrangos ir standartų gausa bei gana paprasti metodai, leidžiantys mikroskopiškai tyrinėti kompiuterinius virusus. Kompiuterinius virusus tyrinėti paprasčiau nei biologinius, nes nereikia mikroskopų, pakanka paprasto kompiuterio.

Makroskopinės virusologijos principai skiriasi nuo mikroskopinių, nes į virusą žvelgia ne iš arti ir neskiria didelio dėmesio viruso struktūrai. Ši metodika nagrinėja virusinę epidemiologiją. Galime suformuoti pagrindinius jos principus ir teiginius:

- Efektyviausias apsaugos metodas – neleisti užsikrėsti;
- Epidemiologinės situacijos valdymas leidžia laiku sustabdyti epidemiją;
- Užkrato šaltinio karantinas stabdo epidemiją;
- Imuninės sistemos gerinimas neleidžia virusams greitai daugintis, mažėja žala.

Remiantis šiais principais, galima kovoti ir su žinomais, ir su nežinomais virusais (analogija biologijoje – SŪRS viruso nemokama sunaikinti, bet epidemija yra sustabdyta), todėl, sparčiai daugėjant kompiuterinių virusų interneto tinkle, ši metodologija tampa vis efektyvesnė ir naudingesnė [5].

Vartotojų elgsenos analize pagrįstos apsaugos sistemos

Šios sistemos yra makroskopinės apsaugos atstovai. Jos renka ir analizuoja vartotojų elgseną: išsiųstus ir gautus laiškus, adresatus ir siuntėjus, siuntimo terminus ir srautus. Analizuodamos šią informaciją priima sprendimus, ar el.laiškas yra pavojingas ir kenkėjiškas, ar tai įprastas vartotojo siunčiamas ar gaunamas laiškas.

Šiuo metu siūlomos metodikos vartotojų elgsenos pokyčiams analizuoti:

- vartotojų grupių metodika (angl. User cliques);
- dažninė Helingerio atstumo metodika (angl. Hellinger distance);
- kaupiamojo plitimo metodika (angl. Cumulative

distribution);

• turinio klasifikavimo metodika (angl. Content based classification);

• sklendinė metodika (angl. Throttling loop).

Taikant *vartotojų grupavimo metodiką* apsaugai nuo kenkėjiškų el.laiškų, sudaromas vartotojo grupių masyvas. Vartotojo grupes sudaro bendradarbių, draugų, šeimos narių ir kt. el.pašto dėžutės. Niekada nebūna situacijos, kad tektų laišką siųsti ir savo vadovui, ir savo žmonai. Atliekant duomenų siuntimo adresatų analizę, galima pastebėti vartotojo elgsenos pasikeitimą, kuriam įtakos galbūt turėjo virusai [6].

D*ažninis Helingerio atstumo modelis* leidžia išmatuoti vartotojo komunikavimo su kitais vartotojais dažnumo pokyčius [7,8].

Kaupiamojo plitimo modelis analizuoja įprastus vartotojų išsiunčiamos informacijos srautus. Kaupdama šią informaciją, sistema gali pastebėti siunčiamos informacijos kiekio pasikeitimus. Šia analize taip pat galima aptikti vartotojo elgsenos pasikeitimus [8].

Turinio klasifikavimo metodika. Analizuojamas tekstinės informacijos turinys ir sudaromi tipinių el.laiškų sudėties vektoriai. Analizuojant tokius vektorius, galima rasti automatiškai virusų kuriamus netipinius laiškus, atskirti tokį srautą nuo tipinio vartotojų kuriamo srauto [8].

Sklendinė metodika analizuoja siuntėjo siunčiamų paketų adresatus. Jei gavėjų adresacija neįprastai kinta, sistema šiek tiek suvėlina paketo perdavimą. Kuo adresacija neįprastesnė ir kuo daugiau siunčiama paketų (virusas plinta), tuo labiau lėtinamas paketų siuntimas. Taip labai sparčiai besidauginantis virusas pradeda pats save slopinti [9].

Virusinių programų epidemijos modeliavimas

Makroskopiniu principu analizuojant kompiuterių virusus, daugiausia dėmesio yra skiriama epidemiologijai. Telekomunikacijų tinkluose virusai sklinda taip pat kaip ir biologinėje terpėje, todėl čia tinka ir biologinių epidemijų modeliai, kurie yra gana gerai ištyrinėti.

Vienas iš svarbiausių aspektų, nagrinėjant epidemiją telekomunikacijų tinkluose, yra jos sukeliama žala. Žalą galime skaičiuoti proporcingai infekuotų mašinų skaičiui. Norėdami įvertinti, kokią įtaką epidemijos maksimumui ir trukmei turi epidemijos gydymo pradžia, modifikuojame standartinį Kermako ir Makendriko SIR tipo epidemijos modelį, kuriame įvertiname infekcijos gydymo pradžios vėlinimą [10]. Čia gydymo intensyvumas yra lygus infekcijos intensyvumui (t-k) metu:

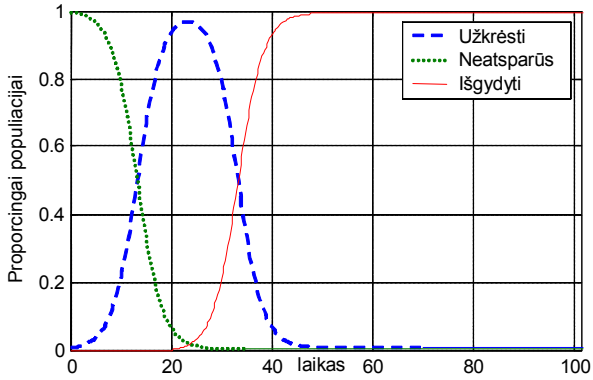
$$\frac{dI(t)}{dt} = \tau \cdot I(t)S(t) - \tau \cdot I(t-k)S(t-k)\,; \qquad (1)$$

$$\frac{dS(t)}{dt} = -\tau \cdot I(t)S(t)\,; \qquad (2)$$

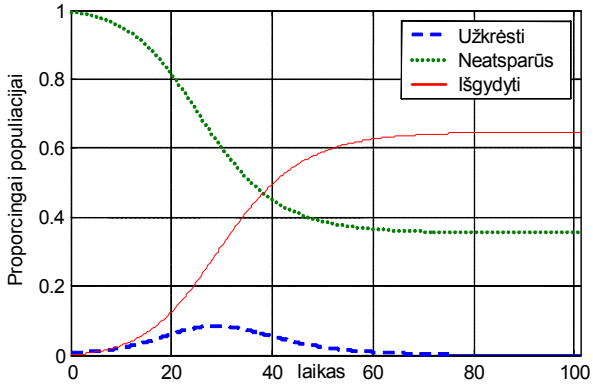
$$\frac{dR(t)}{dt} = \tau \cdot I(t-k)S(t-k)\,; \qquad (3)$$

čia S – Neatsparių mašinų skaičius; I – infekuotų mašinų skaičius; R – išgydytų mašinų skaičius; τ – virusų plitimo spartos koeficientas [0...1]; k – vėlinimo laikas.

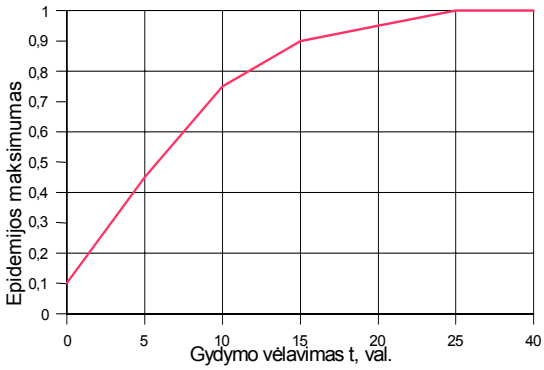
Programa Matlab atlikę modeliavimą, gavome 1, 2, 3 grafikus.



1 pav. Epidemija tinkle, kai virusų gydymas pradedamas po 20 val. nuo epidemijos pradžios (τ = 0,4, k=20)



2 pav. Epidemija tinkle, kai virusų gydymas pradedamas iš karto nuo eidemijos pradžios (τ = 0,4; k=0)



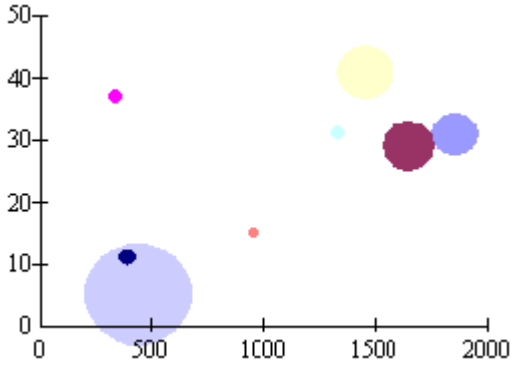
3 pav. Epidemijos maksimumo priklausomybė nuo jos stabdymo pradžios (τ = 0,4)

3 paveiksle matome, kad sparčiai plintant virusui epidemijos maksimumą galima sumažinti tik tuomet, kai gydymas pradedamas nedelsiant (t<20 val.). Būtent šios savybės ir neturi tradicinės mikroskopiniu principu veikiančios apsaugos sistemos.

Intelektuali piktavališko elektroninio pašto stabdymo sistema: eksperimento aprašymas

Vykdant piktavališkų programų epidemijos atpažinimo uždavinį, visų pirma reikia surinkti statistinę informaciją, kurią neuroninis tinklas galės apdoroti. Eksperimentui surinkome 100 el.pašto siuntimo įvykių. 3 paveiksle matyti, jog įvairiais laiko momentais (nuo 400 iki 1900 minutės) siuntėjas siuntė įvairiems gavėjams

skirtingo dydžio laiškus. Apskritimo padėtis x ašyje žymi įvykio laiką, y ašyje – simbolinį gavėjo numerį, apskritimo dydis – laiško priedo dydį.



4 pav. Dešimties el. laiškų be virusų siuntimo įvykiai laikui bėgant

Jei per trumpą laiko tarpą (nuo 5 iki 60 minutės) siuntėjas skirtingiems gavėjams išsiuntė daug vienodo dydžio laiškų, tai suprantama kaip netipinė arba anomali siuntėjo veikla. Žinoma, tai dar nereiškia, jog laiškas siunčiamas viruso, tačiau didelė tikimybė yra. Tokius laiškus galima laikinai sustabdyti ir siuntėjo paprašyti patvirtinti, ar tikrai siunčia jis, o ne virusas. Neuroninio tinklo užduotis šiuo atveju – atskirti tipinius ir netipinius siuntėjų veiksmus.

Eksperimento eiga

Eksperimentui atlikti suformavome FIFO buferį, kuriame laikomi duomenys apie reikiamą skaičių paskutinių išsiųstų laiškų. Buferio ilgis eksperimento metu buvo 5,10 ir 30. Iškėlėme hipotezę, kad iš buferyje esančių el.laiškų neuroninis tinklas gali atpažinti, ar tuos laiškus siunčia vartotojas, ar jie yra generuojami viruso. Ši metodika pasiūlyta HP laboratorijos, tačiau ji statistiniu metodu analizavo žemo lygio TCP protokolo paketus [9].

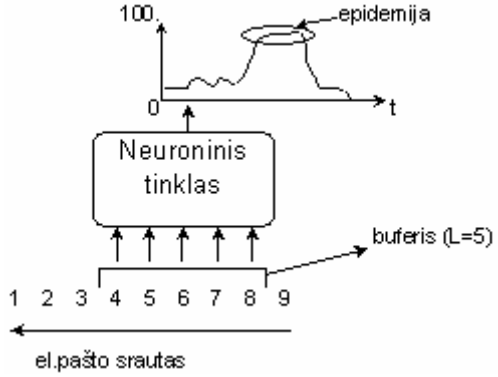
Duomenis analizavome su keturių skirtingų struktūrų neuroniniais tinklais. Eksperimento duomenys, atspindintys normalų sistemos darbą, buvo surinkti iš realios el.pašto programos. Duomenys, atspindintys virusinę infekciją, buvo sugeneruoti remiantis realiomis parametrų kitimo ribomis. Eksperimentu norėjome nustatyti, kokio ilgio buferis turėtų būti naudojamas norint nustatyti kompiuterinio viruso epidemiją bei kokios struktūros neuroninis tinklas šią užduotį atliks geriausiai.

Eksperimentas susidėjo iš trijų dalių:

- neuroninio tinklo mokymas normalią vartotojo veiklą atspindinčiomis parametrų vertėmis;
- neuroninio tinklo mokymas anomalią viruso veiklą atspindinčiomis parametrų vertėmis;
- neuroninio tinklo mokymo testavimas ir normalią, ir anomalią veiklą atspindinčiomis parametrų vertėmis.

Mokydami neuroninį tinklą normalią vartotojo veiklą reprezentuojančiomis parametrų vertėmis, į tinklo įėjimus įvedėme buferyje esančių el.laiškų parametrus. Kaip pageidaujamą neuronų tinklo išėjimo vertę, atspindinčią normalią situaciją, pasirinkome nulį. Mokydami neuroninį tinklą atpažinti anomalią veiką, pageidavome, kad išėjime būtų vertė 100.

Kai buferyje buvo penki el.laiškai, neuroninis tinklas taip pat turėjo penkis įėjimus, tokiu metodu atitinkamai buvo naudojami 10 ir 30 elementų ilgio buferiai.



5 pav. Eksperimento schema

Modeliavimo darbus atlikome su paketu NeuroSolutions. Eksperimente naudojome MLP (angl. *Multilayer perceptron*), SOM (angl. *Self-organizing feature map*), GFF (angl. *Generalized feedforward network*) ir Elman (angl. *Jordan and Elman network*) dirbtinius neuroninius tinklus. Neuroniniams tinklams apmokyti naudojome 1000 ciklų. Neurosolution paketas automatiškai normalizavo visas vertes, įvedamas į neuroninio tinklo įėjimus.

1 lentelėje pavaizdavome dvylikos geriausių eksperimentų rezultatus.

1 lentelė. Eksperimento rezultatai

MLP tinklas

el.laiškų sk.	5	10	30
Mažiausia klaida	**0,15**	**0,02**	**0,01**
Geriausia struktūra	4-4-4	20-10	20-10-4
Pastabos	nest.	nest	stab

SOM tinklas

el.laiškų sk.	5	10	30
Mažiausia klaida	0,15	0,1	0,01
Geriausia struktūra	10-10	10-6-4	20-10-4
Pastabos	nest	stab	greit-stab

GFF tinklas

el.laiškų sk.	5	10	30
Mažiausia klaida	0,2	0,2	0,01
Geriausia struktūra	10-4	10-6-4	20-10-4
Pastabos	lėt-stab	lėt-stab	lėt-stab

Elmano tinklas

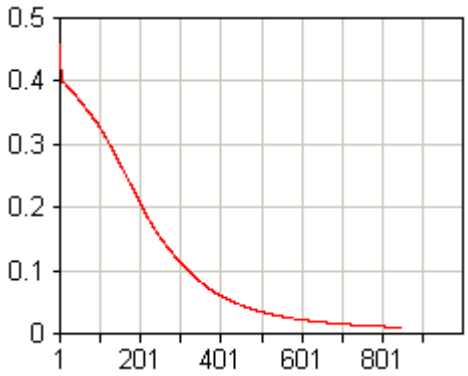
el.laiškų sk.	5	10	30
Mažiausia klaida	0,2	0,05	0,02
Geriausia struktūra	10-4	20-10	20-10-4
Pastabos	lėt-stab	lėt-stab	lėt-stab

Eksperimento metu pirmiausia tikrinome, ar neuroniniam tinklui pakaks 5 paskutinių laiškų duomenų, anomaliniam ir normaliam laiškų srautui atpažinti. Mokymo metu neuroninis tinklas elgėsi labai nestabiliai, įvykdžius 1000 mokymo ciklų, klaidos procentas vis tiek buvo gana didelis – 15 %.

Eksperimento metu, analizuojant 10 laiškų esančių buferyje, rezultatai buvo geresni. Mokymo metu klaidų skaičius mažėjo stabiliau, nors su kai kuriomis neuroninių tinklų struktūromis tinklo mokymas buvo labai nestabilus. Geriausias pasiektas rezultatas, analizuojant 10 paskutinių

laiškų išsiuntimo eilėje, – 2%.

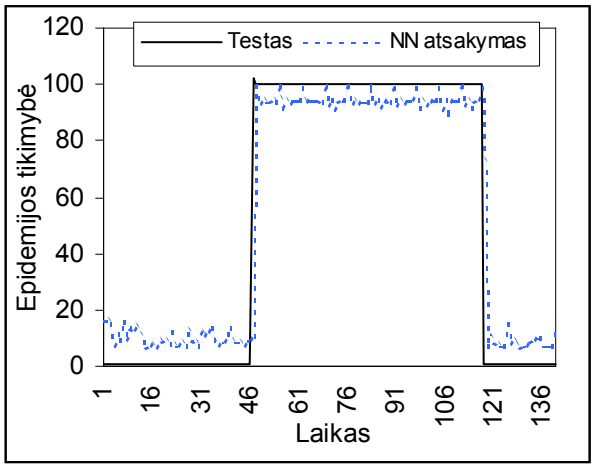
Analizuojant 30 paskutinių laiškų su neuroniniu tinklu, buvo matomas labai stabilus ir greitas neuroninio tinklo mokymas, t. y. ir klaidos mažėjimas. Mokymo metu jau po 800, o su kai kuriomis neuroninių tinklų struktūromis jau po 200 mokymo ciklų, klaidų skaičius sumažėdavo iki 1%. Teoriškai toks tinklas turėtų beveik idealiai atskirti kompiuterinių virusų generuojamą srautą nuo normalaus el.pašto vartotojo generuojamo srauto. Klaidos mažėjimas mokymo metu pavaizduotas 6 paveiksle.



6 pav. Klaidos mažėjimas neuroninio tinklo mokymo metu, analizuojant 30 paskutinių el.laiškų duomenis

Parengto neuroninio tinklo testavimas

Atlikę eksperimentą, pasirinkome tiksliausią metodą ir tinklo dydį rezultatams testuoti. Geriausi rezultai buvo gauti analizuojant 30 laiškų, esančių buferyje. Neuroninis tinklas MLP su 30 įėjimų, 20 neuronų pirmame sluoksnyje, 10 neuronų antrame sluoksnyje, 4 neuronai trečiame sluoksnyje ir 1 neuronas išėjime. Neuroninio tinklo analizei pateikėme normalų srautą, sumaišytą su srautu, kuriame kilo kompiuterių virusų epidemija. Neuroninio tinklo rezultatus grafiškai palyginome su žinomais duomenimis (7 pav.).



7 pav. Testinių ir gautų rezultatų palyginimas

Paveiksle matyti, kaip laikui bėgant normalus srautas (lygis ~0) keičiasi į epidemiją (lygis ~100), kuri po tam tikro laiko baigiasi (lygis ~0). Mokytas neuroninis tinklas, kai epidemijos nėra, taip pat grąžina rezultatą– ~8 – 17 % tikimybę, kad epidemijos nėra. Kai prasideda epidemija, neuroninis tinklas atpažįsta anomaliją ir grąžina rezultatą, kuris su ~90-98 % tikimybe rodo epidemiją.

Taigi neuroniniams tinklams analizuojant duomenis, galima iki 98 % tikslumu nustatyti, kada el.paštą siunčia žmogus, o kada el.laiškus kuria kompiuterinis virusas.

Ši sistema turi trūkumą – kai analizuojama nedaug srauto parametrų – laiškų dydis ir generavimo greitis. Tokia sistema gali įvelti klaidų, jei, pvz.., darbuotojas norės išsiųsti 30 kvietimų į šventę. Šioms problemoms pašalinti taip pat yra metodikos, kurios siūlo sudaryti vartotojų grupes ir jas naudoti kaip papildomą modelio parametrą [6,7,8].

Nors tokios sistemos turi trūkumų, jas naudojant, epidemijos pradžią galima aptikti labai greitai – tereikia virusui sukurti 10 – 30 el. laiškų. Kaip parodė modeliavimas, toks ankstyvas epidemijos aptikimas ir stabdymas yra vienintelis garantas, leisiantis minimizuoti užkrėstų tinklo įtaisų skaičių, o kartu ir epidemijos sukeltus nuostolius.

Išvados

1. Darbe atlikta literatūros analizė parodė, jog dauguma šiuolaikinių virusų plinta el.pašto protokolu, todėl tikslinga kurti el. pašto apsaugos sistemas.
2. Matematiškai modeliuodami įsitikinome, kad, norint kuo labiau sumažinti epidemijos sukeliamus nuostolius, ją reikia atpažinti kuo anksčiau, kol neprasidėjo griūtinis virusų plitimo procesas.
3. Pasiūlyta neuroninių tinklų epidemijos atpažinimo metodika leidžia 2 % tikslumu atpažinti epidemiją iš 10–30 išsiųstų el.laiškų. Praktiškai 30 laiškų buferyje yra labai didelis skaičius, jį reikia kiek įmanoma mažinti.
4. Naudojant šį apsaugos modelį, neuroninis tinklas mokomas konkretaus vartotojo elgsenos ir jai pakitus analizuoja, ar tai epidemija, ar ne. Ši metodika leidžia efektyviai saugoti įvairios elgsenos tipų vartotojus.
5. Norint padidinti modelio tikslumą, reikėtų įvesti papildomą parametrą – vartotojų grupes ar papildomai naudoti turinio klasifikavimo metodus.

Literatūra

1. **Bridwell L.**, ISCA LAbs Virus Prevalence Survey 2002 // Research report. – ISCA Labs, 2002 .– P. 12-20.
2. **MessageLabs Ltd**, Virus Eye Monthly View // Research report. – MessageLabs Ltd, 2003 .– P. 1-2.
3. **Zou C., Lixin G., Gong W., Towsley D.** Monitoring and Early Warning for Internet Worms // Conference CCS'03.- University of Massachusetts at Amherst.– Washington DC, USA, 2003.– P. 7.
4. **Kephart O., Chess M., White R.**, Computers and epidemiology // Research report. - IBM Thomas J. Watson Research Center, 1993 .– P. 20-26.
5. **Kephart J.** A Bilogical Inspired Immune System for Computers // Artificial Life IV: Proceedings of the Fourth International Workshop on the Synthesis and Simulation of Living Systems.- IBM Thomas J. Watson Research Center.– Yorktown Heights. NY, USA, 1994.– P. 130-139.
6. **Bhattacharyya M., Shultz M.G., Eskin E., Hershkop S., Stoflo S.** MET: An experimental System for Malicious Email Tracking // Proceedings of New Security Paradigms Workshop. – New York: Columbia University. (USA), 2002.– P. 1– 12.
7. **Stolfo S., Chan P., Prodromidis A.**, Distributed Data

Minning in Credit Card Fraud Detection // IEEE Inteligent Systems. – Columbia University, 1999. –Vol.14.– No 6.
8. **Stolfo S., Li W., Hershkop S., Wang K.**, Detecting Viral Propagations Using Email Behavior Profiles // Research report. – Columbia University, 2003 .– P. 60.
9. **Williamson M., Twycross J., Griffin J., Norman A.** Virus Throttling // Virus Bulletin–The Pentagon Hewlett Packard, 2003 – Vol.3.– No 3.
10. **Laurutis R.** Neuronų tinklų panaudojimas duomenų apsaugai // Elektronika ir elektrotechnika.– Kaunas: Technologija, 2003. – Nr. 4(46). – P. 61– 64.

Pateikta spaudai 2005 04 11

D. Puniškis, R. Laurutis. Neuroninių tinklų naudojimas kompiuterinių virusų sukeliamoms epidemijoms aptikti // Elektronika ir elektrotechnika. – Kaunas: Technologija, 2005. – Nr. 4(60). –P.28–32.

Kompiuteriniai virusai yra pirmojo dirbtinio intelekto atstovai. Jie gali nevaržomai plisti telekomunikacijų, kompiuterių, o ateityje – ir GSM tinklais. Virusų epidemijos tinkluose vis didėja, kelia grėsmingų QoS problemų, o šiuolaikinės mikroskopinės technologijos nepajėgia efektyviai jų stabdyti. Straipsnyje apžvelgta makroskopinė virusų aptikimo technologija, kuri remiasi vartotojų elgsenos stebėjimu. Analizei naudojami neuroniniai tinklai, kurie yra apmokyti „normalios“ ir „anomalios“ vartotojų elgsenos. Neuroninis tinklas realiu laiku stebi vartotojų elektroninį paštą ir priima sprendimus, ar vartotojas elgiasi įprastai, ar ne. Eksperimentas parodė, kad ši technologija yra efektyvi, tačiau, norint sumažinti klaidingų sprendimų skaičių, ją reikia tobulinti. Il.7, bibl. 10 (lietuvių kalba; santraukos lietuvių, anglų ir rusų k.).

D. Puniskis, R. Laurutis. The Use of Neuron Networks for the Performance of Epidemics Caused by Computer Viruses // Electronics and Electrical Engineering. – Kaunas: Technology, 2005. – No. 4(60). –P.28–32.

Computer viruses are the representatives of the first artificial intelligence. They are able to spread unrestrictedly within the networks of telecommunications, computers and in the near future within GSM. Epidemics caused by viruses in the networks occur more and more frequently bringing ominous problems of computer systems, while modern microscopic technologies are unable to stop them effectively. Microscopic virus detecting technology appealing to the observation of users' behavior is reviewed in the article. Neuron networks are used for analysis as they are indoctrinated with "normal" and "abnormal" behavior of users. The neuron network observes e-mails of the users in the real time and decides whether a user behaves normally or not. It was proved by experiment that this technology is effective but still it needs to be improved in order to reduce the number of invalid decisions. Ill. 7, bibl. 10 (in Lithuanian; summaries in Lithuanian, English and Russian).

Д. Пунишкис, Р. Лаурутис. Использование нейронных сетей для нахождения эпидемий, вызываемых компьютерными вирусами // Электроника и электротехника. – Каунас: Технология, 2005. – № 4(60) – С. 28–32.

Компьютерные вирусы, являющиеся представителями первого искусственного интеллекта, способны беспрепятственно распространяться телекоммуникационными, компьютерными, а в будущем и GSM сетями. Вирусные эпидемии все возрастают, создавая опасные QoS проблемы: тем временем современные микроскопические технологии не в состоянии эффективно их блокировать. В статье представлен обзор макроскопической технологии нахождения вирусов, базирующейся на наблюдениях за поведением потребителей. В анализе используются нейронные сети, которые обучены «нормальному» и «аномальному» поведению потребителей. Нейронная сеть в реальном времени следит за электронной почтой потребителей и принимает решения о том, ведёт ли себя потребитель обычно или нет. Эксперимент показал, что несмотря на то, что данная технология эффективна, её необходимо совершенствовать с целью уменьшения количества ошибочных решений. Ил. 7, библ. 10 (на литовском языке; рефераты на литовском, английском и русском яз.).